

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
Fort Lauderdale Division**

FRANK GANNOZZI, individually and on behalf of all others similarly situated, Plaintiff, v. UKG INC., Defendant.	CASE NO. _____ CLASS ACTION COMPLAINT JURY DEMAND
--	---

CLASS ACTION COMPLAINT

Plaintiff Frank Gannozzi (“Plaintiff”) brings this Class Action Complaint (“Complaint”) on behalf of himself, and all others similarly situated, against Defendant UKG Inc. (“UKG” or “Defendant”) alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE ACTION

1. This class action arises out of Defendant’s failure to properly secure, safeguard, and adequately destroy Plaintiff’s and Class Members’ sensitive personal identifiable information (“PII”) that it had acquired and stored for its business purposes.
2. Defendant’s data security failures allowed a targeted cyberattack to compromise Defendant’s network (the “Data Breach”) that, upon information and belief, contained personally identifiable information of Plaintiff and other individuals (“the Class”). The Data Breach occurred

on or around October 30, 2023.¹ UKG began sending notice letters to Plaintiff and Class Members on January 5, 2024 (“Notice Letter”).²

3. UKG is an HR and workforce management company that provides services to approximately 80,000 organizations.³

4. The PII compromised in the Data Breach included Plaintiff’s and Class Members’ full names, addresses, demographic information, recent salary information, banking and routine information, and Social Security numbers.

5. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves.

6. As a result of the Data Breach, Plaintiff and approximately 45,000 Class Members,⁴ suffered concrete injury in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant’s possession and is

¹ <https://www.jdsupra.com/legalnews/payroll-services-provider-ukg-inc-5587619/> (last visited 02/01/2024).

² *Id.*

³ *Id.*

⁴ According to the report submitted to the Office of the Maine Attorney General, 45,966 persons were impacted in the Data Breach. *See* <https://apps.web.maine.gov/online/aeviewer/ME/40/d00fbf92-37fa-4840-bbc2-418219234ae5.shtml> (last visited 02/01/2024).

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

7. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

8. Defendant failed to adequately protect Plaintiff's and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect the sensitive data of its clients' employees. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even

for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

11. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

18. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

PARTIES

20. Plaintiff, Frank Gannozzi, is an adult individual who at all relevant times has been a citizen and resident citizen of Scarsdale, New York.

21. At all time material hereto, Plaintiff was an employee of Metro-North Railroad ("Metro-North"), a suburban commuter rail service operated by the Metropolitan Transit Authority ("MTA").

22. UKG is the owner of the Kronos system, called UKG Workforce Central, which provides attendance and timekeeping services to the MTA.

23. As an employee of Metro-North, Plaintiff was required to provide his PII to Defendant, including among other things, all his contact information, his Social Security Number, his banking account information, and demographics.

24. Plaintiff diligently protects his PII.

25. Plaintiff is not aware of ever being part of a data breach involving his PII and is concerned that it has now been exposed to bad actors.

26. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his PII multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

27. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

28. Plaintiff greatly values his privacy and would not have provided his PII if he had known that his PII would be maintained using inadequate data security systems. In the course of enrolling in employment and as a condition of employment and/or receiving certain employee benefits, he was required to supply Defendant, directly or indirectly, with his PII—including, but not limited to: his name, address, financial account information, and Social Security number.

29. Plaintiff received the Notice Letter, by U.S. mail, from UKG, dated January 5, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his full name, address, demographic information, recent salary information, Social Security number, and banking and routing information.

30. In response to the Data Breach and the Notice Letter, which instructs Plaintiff to "remain vigilant for incidents of fraud and identity theft by reviewing credit card account

statements and monitoring your credit report for unauthorized activity[,]"⁵ Plaintiff has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, researching the credit monitoring and identity theft protection services offered by Defendant, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect.

31. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

32. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

33. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

⁵ See Notice Letter, a sample copy of which is available at <https://apps.web.maine.gov/online/aeviewer/ME/40/d00fbf92-37fa-4840-bbc2-418219234ae5.shtml>

34. Defendant, UKG, is a Delaware corporation with its principal place of business located at 2250 North Commerce Parkway Weston, FL 33326.

JURISDICTION AND VENUE

35. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds \$5,000,000 exclusive of interest and costs. The number of class members exceeds 100, some of which have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

36. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its business in this District, including decisions regarding the security measures to protect its clients' employees' PII.

37. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiff's and Class Members PII in this District, and has caused harm to Plaintiff and Class Members in this District.

STATEMENT OF FACTS

Background

38. UKG is a “HCM cloud compan[y]” that offers products and services to “80,000+ organizations[.]”⁶

39. Plaintiff and Class Members are current or former employees of Metro-North, which Defendant contracted with to provide payroll and/or other services.

40. Upon information and belief, in the course of collecting PII from its client’s employees, including Plaintiff, Defendant promised to provide confidentiality and adequate security for employee data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

41. Indeed, Defendant provides on its website that:

UKG utilizes physical, technical, and administrative controls and procedures designed to safeguard the information we collect, prevent unauthorized access or disclosure, to maintain data accuracy of your personal information, and to restrict the processing of your personal information as set forth in this Website Notice.

We utilize a variety of physical and logical access controls, firewalls, intrusion detection and prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our Site.

We limit access to your personal information and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your personal information are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.⁷

42. Plaintiff and the Class Members, as former and current employees of Defendant’s clients, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and

⁶ <https://www.ukg.com/about-us> (last visited 02/01/2024).

⁷ <https://www.ukg.com/privacy> (last visited 02/01/2024).

to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

43. In the course of their relationship, employees, including Plaintiff and Class Members, provided Defendant, directly or indirectly, with at least the following PII:

- a. names;
- b. demographic information;
- c. financial account information;
- d. Social Security numbers; and
- e. addresses.

44. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

45. On or about January 5, 2024, Defendant began sending Plaintiff and other Data Breach victims a Notice Letter, informing them that one of the entities with which Defendant regularly shared and allowed to maintain the PII of Plaintiff and Class Members, allowed that PII to be accessed by an unauthorized party:

What Happened? A file that included the personal information of [Metro-North] employees (the "File") was created by UKG in the normal course of providing services to [Metro-North]. On October 30, 2023, UKG became aware that the File was inadvertently exposed to five other customers and promptly opened an investigation.

...

What Information Was Involved? The information in the File included your name, address, demographic information, recent salary information, social security number, and banking and routing information.⁸

⁸ See Notice Letter.

46. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, when Defendant concluded its investigation, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

47. Upon information and belief, the cyberattack was targeted at the PII maintained by Defendant, due to its status as a company that shares, collects, creates, and maintains PII on its computer networks and/or systems.

48. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the PII of Plaintiff and Class Members.

49. As evidenced by the Data Breach's occurrence, the PII was stored on Defendant's network was unencrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

50. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiff and Class Members must, as Defendant's Notice Letter instructs them, "remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity."⁹

51. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it

⁹ *Id.*

entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

52. That Defendant is encouraging Plaintiff and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' PII *was* accessed, thereby subjecting Plaintiff and Class Members to a substantial and imminent threat of fraud and identity theft.

53. Plaintiff's PII was accessed and stolen in the Data Breach and Plaintiff believes his and Class Members' stolen PII is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals

54. Defendant had obligations created by the Federal Trade Commission Act ("FTCA"), contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

55. As explained by the Federal Bureau of Investigation ("FBI"), "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."

56. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁰

¹⁰ *Id.*

57. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹¹

¹¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

58. Given that Defendant was storing the sensitive PII of its clients' employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

59. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of approximately 45,000 employees,¹² including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Plaintiff's and the Class's PII

60. Defendant acquires, collects, shares, and stores a massive amount of PII in the regular course of its business.

61. As a condition of their employment at Defendant's clients, Defendant required Plaintiff and Class Members to entrust it with highly sensitive personal information.

62. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

63. Defendant could have prevented this Data Breach by properly securing and encrypting the files containing the PII of Plaintiff and Class Members.

64. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

¹²<https://apps.web.maine.gov/online/aeviewer/ME/40/d00fbf92-37fa-4840-bbc2-418219234ae5.shtml> (last visited 02/01/2024).

65. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk Because Payroll Companies In Possession of PII Are Particularly Susceptable To Cyber Attacks

66. Defendant's data security obligations were particularly important, given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendant, preceding the date of the breach.

67. Data breaches, including those perpetrated against payroll companies that store PII in their systems, have become widespread.

68. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹³

69. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII it collected and maintained would be targeted by cybercriminals.

70. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities

¹³ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last visited 02/01/2024).

that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁴

71. Defendant knew and understood unprotected or exposed PII in the custody of payroll companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

72. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

73. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

74. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

75. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

¹⁴ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited 02/01/2024).

76. As a payroll company in custody of its clients' current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

77. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁵ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁶

78. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁷

¹⁵ 17 C.F.R. § 248.201 (2013).

¹⁶ *Id.*

¹⁷ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited 02/01/2024).

79. For example, PII can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁸

80. Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.

81. Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁹

82. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁰

83. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against

¹⁸ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

¹⁹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited 02/01/2024).

²⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited 02/01/2024).

the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

84. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²¹

85. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security numbers and names.

86. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²²

87. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

88. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered,

²¹ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited 02/01/2024).

²² Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited 02/01/2024).

and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²³

Defendant Fails To Comply With FTC Guidelines

89. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

90. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²⁴

91. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁵

²³ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited 02/01/2024).

²⁴ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited 02/01/2024).

²⁵ *Id.*

92. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

93. The FTC has brought enforcement actions against payroll companies for failing to protect employee data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

94. Defendant failed to properly implement basic data security practices.

95. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its clients' employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

96. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its clients' current and former employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails To Comply With Industry Standards

97. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

98. Several best practices have been identified that a minimum should be implemented by payroll companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

99. Other best cybersecurity practices that are standard for payroll companies include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

100. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards for payroll companies. Upon information and belief, Defendant failed to comply with at least one—

—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Breached Its Duty to Safeguard Plaintiff's and Class Members' PII

102. In addition to its obligations under federal and state laws, UKG owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. UKG owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members

103. UKG breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. UKG's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect its clients' employees' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to sufficiently train its employees regarding the proper handling of its clients' employees' PII;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

- f. Failing to adhere to the industry standards for cybersecurity as discussed above;
and
- g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

104. UKG negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access the unsecured and unencrypted PII of Plaintiff and Class Members.

105. Had UKG remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

COMMON INJURIES & DAMAGES

106. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk Of Identity Theft

107. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

108. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

109. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

110. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

111. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

112. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.²⁶

113. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

114. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

²⁶ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

115. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

116. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

117. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

118. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

119. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant’s Notice Letter instructs them, “remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.”²⁷

120. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, researching the credit monitoring and identity

²⁷ See Notice Letter.

theft protection services offered by Defendant, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

121. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."²⁸

122. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁹

Diminution Value Of PII

123. PII is a valuable property right.³⁰ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

²⁸ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>. (last visited 02/01/2024).

²⁹ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

³⁰ See, e.g., T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

124. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of PII often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

125. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³¹

126. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{32,33}

127. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁴

128. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.³⁵

129. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property,

³¹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³² <https://datacoup.com/>

³³ <https://digi.me/what-is-digime/>

³⁴ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

³⁵ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

130. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

131. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially over forty thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

132. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

133. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

134. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

135. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

136. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of The Benefit Of The Bargain

137. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When submitting PII to Defendant under certain terms through a job application and/or onboarding paperwork, Plaintiff and other reasonable employees understood and expected that Defendant would properly safeguard and protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received an employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant's clients.

CLASS ACTION ALLEGATIONS

138. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

139. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All persons in the United States whose PII was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant in January 2024 (the "Class").

New York Subclass

All persons in the state of New York whose PII was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant in January 2024 (the "New York Subclass").

140. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

141. Plaintiff hereby reserves the right to amend or modify the Class and/or New York Subclass definitions with greater specificity or division after having had an opportunity to conduct discovery.

142. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, according to the report submitted to the Maine Attorney General, the Class consists at least 45,000 persons whose data was compromised in Data Breach.³⁶

143. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

³⁶ <https://apps.web.maine.gov/online/aewiewer/ME/40/d00fbf92-37fa-4840-bbc2-418219234ae5.shtml> (last visited 02/01/2024).

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- f. Whether Defendant breached its duty to Class Members to safeguard their PII;
- g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

- n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

144. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

145. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

146. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' PII was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

147. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

148. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

149. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

150. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and notified by Defendant.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

151. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 150.

152. Defendant required Plaintiff and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits at Defendant's clients.

153. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its clients, which solicitations and services affect commerce.

154. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

155. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

156. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to give prompt notice to those affected in the case of a data breach.

157. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

158. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and those of its partners, and the personnel responsible for them, adequately protected the PII.

159. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of their employment and/or receiving certain employment-related benefits at Defendant's clients.

160. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

161. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

162. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

163. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

164. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

165. Defendant breached its duties, pursuant to the FTCA and other applicable standards, and thus was negligent by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Allowing unauthorized access to Class Members' PII;
- d. Failing to detect in a timely manner that Class Members' PII had been compromised;
- e. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,
- f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

166. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

167. Plaintiff and Class Members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

168. Defendant's violations of Section 5 of the FTCA constitute negligence.

169. The FTC has pursued enforcement actions against payroll companies, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

170. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

171. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the payroll industry.

172. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

173. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

174. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

175. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

176. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

177. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

178. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

179. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

180. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

181. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs

associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

182. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

183. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

184. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

185. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

186. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach Of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

187. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 150.

188. Defendant entered into written contracts with its clients, including Metro-North, to provide payroll and/or other services.

189. As part of that agreement, Defendant agreed to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

190. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, the clients' current and former employees—Plaintiff and Class Members—would be harmed.

191. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

192. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

193. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

194. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 150.

195. Plaintiff brings this claim in the alternative to his breach of third-party beneficiary claim above.

196. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing their valuable PII to Defendant.

197. Plaintiff and Class Members provided Defendant their PII, directly or indirectly, on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

198. Defendant benefited from receiving Plaintiff's and Class Members' PII through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

199. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

200. Because all PII provided by Plaintiff and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the PII it collected from its clients' current and former employees was inherent to their relationship.

201. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

202. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

203. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII.

204. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

205. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

206. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

207. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

208. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

209. Plaintiff and Class Members have no adequate remedy at law.

210. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury as described herein.

211. Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV
Violation of the New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the New York Subclass)

212. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 150 and brings this claim on behalf of himself and the New York Subclass (the "Class" for the purposes of this count).

213. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- a. Misrepresenting material facts to Plaintiff and the Class by representing that it would maintain adequate data privacy and security practices and procedures to

safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

- b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' PII;
- c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' PII;
- d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,
- e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

214. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the PII entrusted to it by Class Members, and that risk of a data breach or theft was highly likely.

215. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security and made affirmative representations regarding its data security commitments and practices.

216. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendant's network and aggregation of PII.

217. The representations upon which current and former employees at Defendant's clients (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of PII), and current and former employees (including Plaintiff and Class Members) relied on those representations to their detriment.

218. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information.

219. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

220. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing employment services to its clients in the State of New York.

221. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

222. Plaintiff and Class Members were injured because:

- a. Plaintiff and Class Members would not have accepted employment at Defendant's clients, had they known the true nature and character of Defendant's data security practices;

- b. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and
- c. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

223. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and the Class Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

224. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

225. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed employment decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive, and

unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

226. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

227. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

228. Also as a direct result of Defendant's violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthening their data security systems and monitoring procedures; (ii) submitting to future annual audits of those systems and monitoring procedures; and (iii) immediately providing adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class and New York Subclass, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed

in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
- xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

- E. For an award of punitive damages, as allowable by law;
- F. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: February 1, 2024

Respectfully submitted,

/s/ Jeff Ostrow
Jeff Ostrow (FBN 121452)
KOPELOWITZ OSTROW, P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-332-4200
ostrow@kolawyers.com

Andrew J. Shamis, Esq. (FBN 101754)
SHAMIS & GENTILE P.A.
ashamis@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Telephone: 305-479-2299

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiff and the Proposed Class